JumpStart Guide to Investigations and Cloud Security Posture Management in AWS

Kyle Dickinson

SANS

A SANS Whitepaper

JumpStart Guide to Investigations and Cloud Security Posture Management in AWS

Written by **Kyle Dickinson**

November 2019

Sponsored by:

AWS Marketplace
in conjunction with
Barracuda

Introduction

"Cloud security posture management" (CSPM) is a relatively new term when it comes to security capabilities. In the past couple of years, CSPM has gained popularity as organizations move to a cloud-first mentality, shared by many. CSPM allows us to monitor our cloud environment, manage the risk, maintain visibility and understand the operations within an organization's AWS accounts. With CSPM's unique ability to monitor all regions in an AWS account without excessive overhead configuration costs, users can expect scalable deployment and rapid adoption of AWS.

CSPM enables efficient investigations because it centralizes data sources that provide operational and security insight. As we talk about the different considerations throughout this paper, we highlight the tactics that can aid in an investigation.

Understanding Your Needs

When an organization moves to the cloud, the security team needs visibility into its AWS accounts, which can be a complex undertaking. Multiple account strategies are being leveraged by organizations to separate sandbox, development and production accounts, or for sensitive workloads to limit the blast radius. This approach presents a unique opportunity for organizations to understand how they scale with this growth.

Implementation Options in AWS

Before jumping into CSPM, review the different implementation options available to you through AWS: SaaS, licensing, managed services and consulting partner opportunities. Once you've made the decision on how you want to proceed, you'll want to build your business case for that implementation option.

SaaS Platform

Most if not all CSPM platforms are SaaS, which allows security organizations to focus on risk management incident response without the administrative overhead of managing hardware network connectivity and configuration files (with the exception of the limited configuration required for the platform).

Licensing Options

Obtaining any licenses for a CSPM can be done through multiple channels. One may fit your organization better than another. CSPMs can be licensed through AWS Marketplace, bring-your-own-license (BYOL), and private sales via vendors or channel partners. When licensing a CSPM, determine whether the license count applies to the number of AWS accounts being monitored or the amount of resources within your AWS accounts.

Managed Services

Managed security service providers (MSSP) can offer implementation of a CSPM into your organization's environment. An MSSP includes AWS security subject-matter experts, the capability to rapidly integrate existing AWS accounts, and training and customization of the CSPM for your organization. If your organization does not have suitable resources to maintain a CSPM, try leveraging services that can support the initial implementation and cater to the unique aspects of your organization.

Consulting Partner Private Offers (CPPO)

Customers can also engage through CPPO to work directly with trusted advisors to select and configure CSPM solutions from AWS Marketplace. As organizations build out their cloud and cloud security strategy and plan, they may want to consider working with partners to accelerate their efforts or fill any gaps in knowledge or resources that are identified. All consulting partners may extend AWS Marketplace third-party solutions directly to customers through CPPO. Not every organization will be able to find resources with deep cloud experience, and even experienced cloud technologists may have experience only in specific industries or with certain cloud vendors.

Needs and Capabilities: The Business Case for CSPM in the Cloud

With the shared responsibility model of cloud services, certain methodologies of investigations will differ, and the datasets leveraged also change. With the scalability of AWS, CSPMs will aid investigations, incident response and security operations. In this section, we cover key solutions and capabilities an organization will need to use cloud security posture management resources to assist in conducting investigations in AWS.

Business Case for Investigations

The need: Provide an organization the capability to conduct inquiries in a methodical manner.

Capabilities

- Understanding of cloud technologies
- Experience in evidence handling and report writing

Business Case for CSPM

The need: A platform to consolidate a company's AWS presence

Capabilities

- Tracks who is making modifications within AWS accounts
- Performs continuous compliance checks to understand risk being introduced to a cloud footprint
- Provides reports for executives
- Inventories assets to better understand infrastructure for operations
- Provides feedback on risks associated with workloads being developed

General CSPM and Investigation Considerations

In the growing market of CSPM providers, each has unique capabilities. The following sections address the business, technical and operational aspects to consider when evaluating a CSPM, and how to evaluate your ability to conduct an investigation.

CSPM Considerations

Regardless of the vendor(s) you choose to use for CSPM, you should review a variety of business, technical and operational considerations.

Business Considerations

	Consideration	Details
	Data retention	How long will indexed data from your cloud accounts be stored by the CSPM vendor? Do the retention policies align with your organization's approach? If you discontinue using the vendor, what will happen to your data in their systems? **Evaluate:** • Contract language • How data is anonymized for usage outside your tenant
	Licensing	Understand the cost associated with bringing a CSPM to your organization and how the CSPM licenses their platform. **Evaluate:** • Per account monitored • Per resource monitored • Per feature used
	Responsibility	Because CSPM is a SaaS platform, administrative overhead should be minimal; however, there is still administrative responsibility on the consumer. **Evaluate:** • Internal knowledge set • Teams that are connected with security efforts

Technical Considerations

	Consideration	Details
	Account integration	Evaluate how a CSPM authenticates to an organization's existing cloud footprint to determine whether it introduces risk. What changes must be configured within the account for the platform to function? **Evaluate:** • Authentication process for a cloud account • Resources that need to be configured for the CSPM to function
	Authentication	Secure access to the CSPM, use authentication standards and ensure access can be easily disabled when a user is no longer authorized to access the CSPM. **Evaluate:** • Federated identity integration • Authentication standards supported (SAML and OpenID, for example)
	API	APIs allow for access to functionality and extend CSPMs further by allowing programmatic access to data. **Evaluate:** • Documentation • Access controls specifically for API access, and access keys • Logging

Operational Considerations

	Consideration	Details
	Functionality monitoring	Understand your CSPM provider's connectivity to your AWS account(s). If the integration fails, it can be detrimental to functionality. **Evaluate:** • If the communication between a platform and account disconnects, how is the security team notified? • Is there any mechanism to pinpoint the failure for troubleshooting?
	Custom alerts	CSPM tools come with pre-built alerts. However, your organization may have unique use cases requiring custom alerts. **Evaluate:** • Ease of alert creation • Customization options - Severity - Auto-remediation
	Reporting and dashboards	In order to articulate the security posture, executives may require different reports—or your security organization may have to produce proof of attestation. Understanding whether risk is increasing or decreasing can also aid the security team and developers in understanding any risk being removed or introduced from cloud service providers. **Evaluate:** • Report customization and generation • Dashboard customization • Ability to export metrics for more granular analytic tools

Investigation Considerations

As you select the technologies you want to use to conduct an investigation, think through some general business, technical and operational considerations that are associated with investigations in a cloud environment. The following sections highlight many of these considerations.

Business Considerations

	Consideration	Details
	Legal	When performing an investigation, investigators should understand the organization's policies in place, and which data they're allowed to access as part of their investigation. **Evaluate:** • Company's acceptable-use policy • Authority to request an investigation
	Organizational	Those performing investigations should have a strong understanding of the technical controls in place that they're able to leverage. **Evaluate:** • Familiarity of technologies that are involved with the investigation

Technical Considerations

	Consideration	Details
	Evidence storage	Review where the evidence will be stored and ensure strict access controls. **Evaluate:** • Access controls to evidence storage • Audit logging availability to understand chain of custody
	Integrity checking	Investigators should be able to verify the integrity of the data to ensure that logs have not been tampered with. **Evaluate:** • How can you validate the integrity of the data being leveraged for evidence? - AWS CloudTrail integrity validation is an example.

Operational Considerations

	Consideration	Details
	Game days	With the dynamic nature of cloud service providers, investigators should perform dry runs of mock scenarios to keep skills relevant. **Evaluate:** • Frequency of dry runs • Knowledge gaps

AWS Implementation Considerations

The general considerations discussed so far can help organizations lay the groundwork as well as secure funding and support for CSPM and investigations. Now let's take a more detailed look at some specific considerations an organization will need to evaluate before implementing these solutions in AWS.

CSPM

	Consideration	Details
	Asset inventory	To ensure an organization's ability to manage its security posture, it must have tools available to inventory all running endpoints on AWS accounts. **Evaluate:** • What services does the CSPM tool evaluate to create an inventory? • Can you view inventory of systems that may no longer exist?
	Deployment	When deploying a CSPM system, understand how to continuously integrate it while adding new accounts and maintaining existing ones. Know the overhead required. **Evaluate:** • What services in the AWS account need to be configured for the CSPM tool to function properly? • How does the CSPM tool authenticate to an AWS account to monitor? • What does the configuration process entail?

	Consideration	Details
	Feedback loops for developers	DevOps principles encourage leveraging feedback loops so development teams can understand what is occurring with their workload. **Evaluate:** • How can alerts be delivered? • Does the CSPM tool offer integrations to communicate to third-party tools such as a ticketing system, SIEM or data analytics tool?
	Functionality monitoring	If the integration is failing, you need to understand the functionality of your CSPM provider's connectivity to your AWS account(s). **Evaluate:** • If the connection between a platform and account fails, how is the security team notified? • Will any notification tell you which component of ingestion has failed? • If the connection is still active but the CSPM tool is malfunctioning, how can you identify the issue(s)?

Investigations

	Consideration	Details
	Authentication and authorization	In order to properly investigate, the investigator/analyst must have access to the AWS account(s). **Evaluate:** • What type of authentication will be used: local IAM, federated or cross-account role authentication? • What level of access will be provided: root, admin, privileged, read only?

Making the Choice

In summary, the key considerations for conducting investigations and implementing a CSPM solution are:

- Reporting
- Third-party integrations
- Ability to customize alerts
- Deployment
- Scaling
- Vendor support models

Automate the Scaling of the CSPM Solution

As an organization's AWS footprint grows, automate:

- The deployment of required resources to an AWS account for the CSPM tool to function
- The onboarding of the AWS accounts into the CSPM solution

This automation will allow the security team and the developers to ensure the CSPM tool's growth and aid in the success of maintaining visibility into your AWS environment.

Conclusion

CSPM is a crucial step toward securing an organization's presence in a rapidly changing landscape. Pairing a CSPM with security teams and extending the CSPM for developers to leverage as a feedback loop will enable organizations to begin embedding security into the development process. Keep in mind that when operating in AWS, security becomes everyone's responsibility—and CSPMs make this process easier.

About the Author

Kyle Dickinson teaches SANS SEC545: Cloud Security Architecture and Operations and has contributed to the creation of other SANS courses. He is a cloud security architect for one of the largest privately held companies in the United States. As a strategic consultant in his organization, Kyle partners with businesses in various industries to better understand security and risks associated with cloud services. He has held many roles in IT, ranging from systems administration to network engineering and from endpoint architecture to incident response and forensic analysis. Kyle enjoys sharing information from his experiences of successes and failures.

Sponsor

SANS would like to thank this paper's sponsor:

in conjunction with

About Barracuda

Barracuda Networks, Inc. is a company providing security, networking and storage products based on network appliances and cloud services. The company's security products include products for protection against email, web surfing, web hackers and instant messaging threats such as spam, spyware, trojans, and viruses. The company's networking and storage products include web filtering, load balancing, application delivery controllers, message archiving, NG firewalls, backup services and data protection.

Last Updated: November 21st, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Bangalore 2019	Bangalore, IN	Nov 25, 2019 - Nov 30, 2019	Live Event
SANS Cyber Threat Summit 2019	London, GB	Nov 25, 2019 - Nov 26, 2019	Live Event
SANS Nashville 2019	Nashville, TNUS	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS San Francisco Winter 2019	San Francisco, CAUS	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS Security Operations London 2019	London, GB	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS Paris December 2019	Paris, FR	Dec 02, 2019 - Dec 07, 2019	Live Event
SANS Frankfurt December 2019	Frankfurt, DE	Dec 09, 2019 - Dec 14, 2019	Live Event
SANS Cyber Defense Initiative 2019	Washington, DCUS	Dec 10, 2019 - Dec 17, 2019	Live Event
SANS Austin Winter 2020	Austin, TXUS	Jan 06, 2020 - Jan 11, 2020	Live Event
SANS Threat Hunting & IR Europe Summit & Training 2020	London, GB	Jan 13, 2020 - Jan 19, 2020	Live Event
SANS Miami 2020	Miami, FLUS	Jan 13, 2020 - Jan 18, 2020	Live Event
Cyber Threat Intelligence Summit & Training 2020	Arlington, VAUS	Jan 20, 2020 - Jan 27, 2020	Live Event
SANS Tokyo January 2020	Tokyo, JP	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Amsterdam January 2020	Amsterdam, NL	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Anaheim 2020	Anaheim, CAUS	Jan 20, 2020 - Jan 25, 2020	Live Event
MGT521 Beta Two 2020	San Diego, CAUS	Jan 22, 2020 - Jan 23, 2020	Live Event
SANS Las Vegas 2020	Las Vegas, NVUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Vienna January 2020	Vienna, AT	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS San Francisco East Bay 2020	Emeryville, CAUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Security East 2020	New Orleans, LAUS	Feb 01, 2020 - Feb 08, 2020	Live Event
SANS London February 2020	London, GB	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Northern VA - Fairfax 2020	Fairfax, VAUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS New York City Winter 2020	New York City, NYUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Dubai February 2020	Dubai, AE	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS Brussels February 2020	Brussels, BE	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS San Diego 2020	San Diego, CAUS	Feb 17, 2020 - Feb 22, 2020	Live Event
Open-Source Intelligence Summit & Training 2020	Alexandria, VAUS	Feb 18, 2020 - Feb 24, 2020	Live Event
SANS Tokyo November 2019	OnlineJP	Nov 25, 2019 - Nov 30, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced